With dispersed workforces and exploding data volumes, content security and governance needs to be a strategic priority for enterprises looking to compete in the digital economy.

Content Security and Governance for the Hybrid Workforce

June 2021

Written by: Holly Muscolino, Research Vice President, Content Strategies and the Future of Work, and Ryan O'Leary, Esq., Research Manager, Privacy and Legal Technology

Introduction

Even prior to the global pandemic, the digital economy required workers to operate as dynamic and reconfigurable outcome-focused teams that could quickly adapt to business demands and new market requirements — at any time and from any physical location. This trend was accelerated by the pandemic, when nearly 40% of the world's workforce became remote practically overnight.

We now know that this trend will continue. Just under half of all respondents in a recent IDC survey agreed that remote and hybrid work models will become an embedded part of accepted work practices across many industries (see Figure 1). Top priority areas for technology investment over the next two years include workplace transformation programs to ensure long-term resilience and business success (55% of respondents) and security, privacy, and compliance technologies to improve risk posture (59% of respondents).
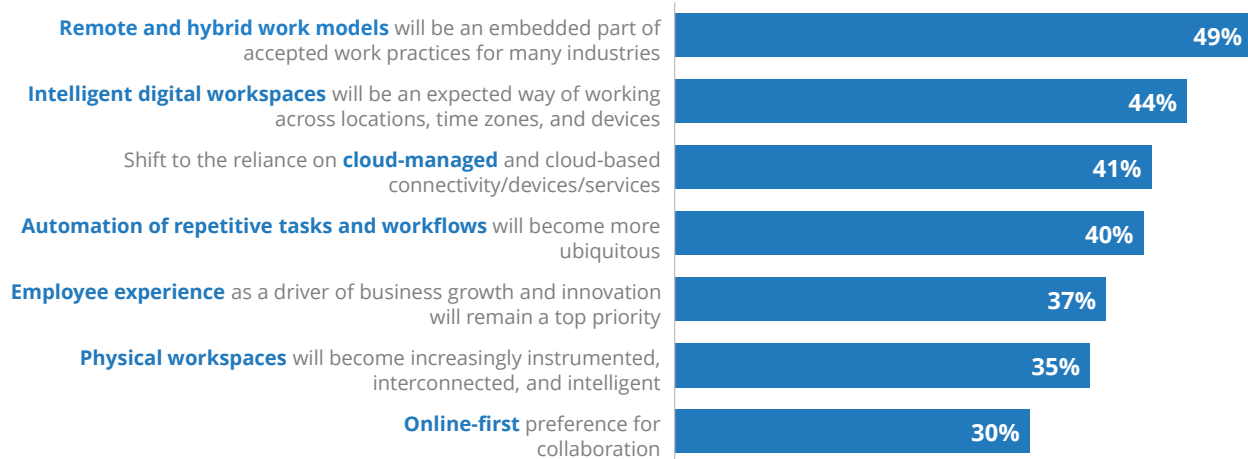
AT A GLANCE

KEY STATS

» Productivity data, which includes content and collaboration data as well as email and productivity documents or files, will grow from 5.5ZB in 2020 to more than 23ZB in 2025 at a compound annual growth rate of more than 33%.

» Organizations average 135 data subject access requests per month and spend around $200,000 a month to fulfill them.

FIGURE 1: *Pandemic-Era Technology Advances That Will Endure*

Q *Which work practices and technology advances emerging from the pandemic are most likely to endure?*

Work practice / technology advance	%
Remote and hybrid work models will be an embedded part of accepted work practices for many industries	49%
Intelligent digital workspaces will be an expected way of working across locations, time zones, and devices	44%
Shift to the reliance on **cloud-managed** and cloud-based connectivity/devices/services	41%
Automation of repetitive tasks and workflows will become more ubiquitous	40%
Employee experience as a driver of business growth and innovation will remain a top priority	37%
Physical workspaces will become increasingly instrumented, interconnected, and intelligent	35%
Online-first preference for collaboration	30%

n = 738

Source: IDC's Future Enterprise Resiliency and Spending Survey — Wave 2, February 2021

Content is at the heart of any business and many business processes, and secure, agile access to all services associated with the content life cycle is crucial for all workers, regardless of their role and location, and across all industries and company sizes.

Content Challenges

Content sprawl is accelerating. According to IDC's *Worldwide Global DataSphere Forecast, 2021–2025*, productivity data, which includes content and collaboration data as well as email and productivity documents or files, will grow from 5.5ZB in 2020 to more than 23ZB in 2025 at a compound annual growth rate exceeding 33%. In a recent IDC survey, 33% of respondents indicated that the sheer volume of content was a top challenge while they adopted technology to digitize and transform their document workflows (*U.S. Enterprise Content Strategies – Use Cases Survey*, December 2020, n = 608).

Data sprawl and data growth are becoming serious challenges for organizations. Global data privacy regulations require organizations to find and produce data related to specific individuals when it is requested. This becomes challenging organizationally when data grows and spreads out among hundreds of enterprise applications. The sheer volume of legacy systems, data, and newer cloud-based systems is difficult to manage. It is further compounded by the volume of requests that enterprises are receiving. In another recent IDC survey, organizations indicated that they are averaging 135 data subject access requests per month and spending around $200,000 a month to fulfill them (*Data Protection and Privacy Survey,* December 2020, n = 336). Subject rights request fulfillment is still a highly manual process and requires visibility into the enterprise datasphere.

Data privacy and other compliance challenges are driving a content security and governance revolution and shifting more toward continuous data intelligence. Enterprises of all sizes are no longer satisfied with data stores and data tools that are updated on a monthly or a yearly cadence and instead are investing in data discovery and mapping tools that can provide continuous insights into how data is flowing through their organization. Complex compliance challenges including data residency mandates require businesses to have more granular information on where data is located physically and who is accessing it. This is even more challenging for midmarket enterprises. Midmarket enterprises have fewer resources and less bandwidth to address their technological complexity and require even more visibility, as loss events have a much more significant impact on midmarket companies' bottom lines. Enterprises need to accomplish these goals while enabling their workforce.

To ensure optimal, secure access to corporate resources, organizations are developing and adopting intelligent digital workspaces — environments that are device and location agnostic and offer personalized (or at least customized) secure federated access to the resources workers require to get their jobs done, including federated content, vital applications, and key collaborators.

Benefits of Securing, Governing, and Transforming Content Workflows

To compete in the digital economy, where data is often at the core of enterprise processes, enterprises need to have quality data that is optimized. Visibility into the datasphere of the enterprise is essential. Gaining visibility into enterprise data is made more complex by disorganized data that is not easily searchable. Organizations that do not focus on content security and governance can find themselves drowning in redundant, obsolete, trivial, and stale (ROTS) data. Enterprises need to clean, organize, and govern their data. Significant technological investment is required to better organize and understand the data that they have as well as where the data is stored and who is accessing it. Technology coupled with routine purging of ROTS data is key to removing the noise and limiting the risks faced by organizations.
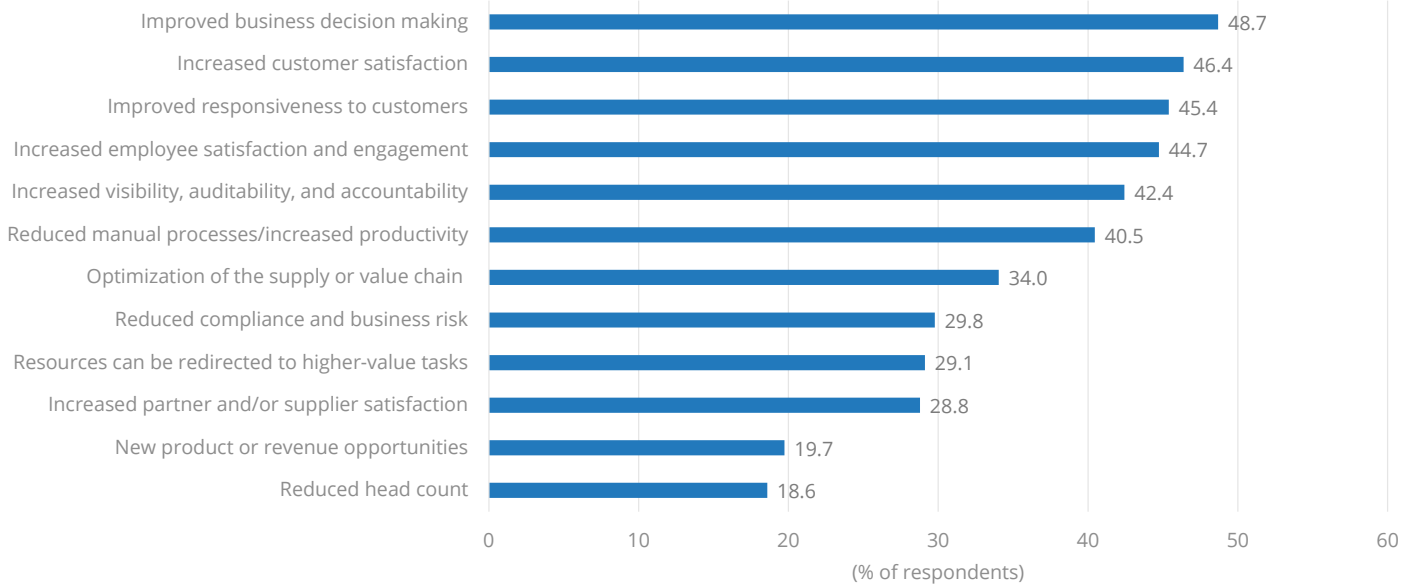
Threat actors are breaching organizations at a staggering rate. According to IDC's 2020 *Data Protection and Privacy Survey,* 60% of respondents reported dealing with malware-infected endpoints on a quarterly basis. In that same survey, 53.5% of respondents reported experiencing ransomware incidents quarterly, and another 57.2% indicated that they experience a loss/leak of more than 1,000 records of personally identifiable information (PII) yearly. Organizations that clean out their ROTS data have less data that can be breached or impacted by malware and ransomware. Further, organizations with visibility into who is accessing the data can better ensure whether improper access is occurring.

Security incidents and breaches are costly. But if a content security and governance program is run properly, then a lot of the risk can be eliminated, increasing the profitability and revenue numbers for the organization. Protecting the organization will mitigate some risk and in turn possibly increase the company's bottom line, but the reputational impacts can have an even deeper effect.

As such, reputation and trust can drive consumers to or away from a business. Consumers more frequently make purchase decisions based on trust. Inadequate content security and governance measures can lead to lapses in that trust. Organizations that devote resources, invest in technology, and engender trust in their brands stand to gain. Protecting the trust and goodwill associated with a brand needs to be a key strategic investment in any digital enterprise.

In addition, organizations that transform document processing see improved decision making, increased employee and customer satisfaction and engagement, reduced manual processes, and improved productivity, visibility, auditability, and accountability (see Figure 2).

FIGURE 2: *Benefits of Transformed Document Processes*

Benefit	% of respondents
Improved business decision making	48.7
Increased customer satisfaction	46.4
Improved responsiveness to customers	45.4
Increased employee satisfaction and engagement	44.7
Increased visibility, auditability, and accountability	42.4
Reduced manual processes/increased productivity	40.5
Optimization of the supply or value chain	34.0
Reduced compliance and business risk	29.8
Resources can be redirected to higher-value tasks	29.1
Increased partner and/or supplier satisfaction	28.8
New product or revenue opportunities	19.7
Reduced head count	18.6

n = 608

Source: IDC's U.S. Enterprise Content Strategies — Use Cases Survey, December 2020

Consider Egnyte for Content Security and Governance

Egnyte provides a unified content security, compliance, and collaboration solution for multicloud businesses of all sizes. Egnyte's solution helps organizations perform the following functions: content life-cycle management, sensitive content discovery, compliance and audit, exposure detection and alerting, controlled sharing to/from any device, and insider threat protection.

The Egnyte solution is designed to be simple and turnkey, reportedly working well with on-premises and multicloud environments without the need for administrative overhead or additional IT staff. The company offers a tight integration with the most popular productivity applications, including Microsoft Office 365 and Google Workspace, as well as on-premises and cloud storage repositories. Egnyte's solution is designed to simplify and strengthen content security, privacy, compliance, and collaboration for distributed teams and the new hybrid workforce.

Challenges

According to a recent IDC survey, 35% of organizations globally are still focused on the basics of business continuity and cost optimization (*Future Enterprise Resiliency and Spending Survey — Wave 3,* April 2021, n = 854). Investment in the transformation of content workflows may be competing with other business priorities in those organizations, though content workflow solutions will certainly contribute to continuity and future resiliency. In addition, transitioning to a new content security and governance solution may seem daunting to large enterprises that house massive amounts of content in on-premises repositories. Additional challenges to adoption may be siloed organizations and disparate legacy applications that do not integrate.

Egnyte predominantly competes with Microsoft and its full suite of offerings, as well as niche governance and compliance solution providers, which typically service large enterprises. While Egnyte integrates well with Microsoft and its add-ons to help eliminate administrative overhead, its lack of brand recognition may inhibit the company from penetrating the larger enterprise market.

Conclusion

The future of enterprise is digital. Digital enterprises have disparate employee bases that are working from almost anywhere, including centralized offices. With dispersed workforces and exploding data volumes, content security and governance needs to be a strategic priority for enterprises that are looking to compete in the digital economy. Visibility into data, security, and compliance challenges requires organizations to protect their brands and engender them with trust by improving content governance.

About the Analysts

Holly Muscolino, *Research Vice President, Content Strategies and the Future of Work*

Holly Muscolino is the Research Vice President, Content Strategies and the Future of Work, responsible for research related to innovation and transformation in content solutions, including intelligent document processing, signature, and other content workflow services. Ms. Muscolino's core coverage also includes work transformation and the role of technology in driving the Future of Work.

Ryan O'Leary, Esq., *Research Manager, Privacy and Legal Technology*

Ryan O'Leary is a Research Manager in IDC's Security and Trust research program covering Privacy and Legal Technology. In this role, Mr. O'Leary leverages his legal experience to provide perspective on changes in laws, shifting regulation, and other market forces that affect technology decision making today for both law firms and corporations.

MESSAGE FROM THE SPONSOR

About Egnyte

Egnyte provides the only unified cloud content governance solution for collaboration, data security, compliance, and threat prevention for multicloud businesses. More than 17,000 organizations trust Egnyte to reduce risks and IT complexity, prevent ransomware and IP theft, and boost employee productivity on any app, any cloud, anywhere. For more information, visit www.egnyte.com.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.

140 Kendrick Street

Building B

Needham, MA 02494, USA

T 508.872.8200

F 508.935.4015

Twitter @IDC

idc-insights-community.com

www.idc.com

≋IDC